Spring 5-1-2018

Security Analysis of the UConn Husky One Card

Trevor Phillips
trevor.j.phillips@uconn.edu

Security Analysis of the UConn Husky One Card

Undergraduate Honors Thesis

Trevor Phillips
Computer Science & Engineering
University of Connecticut - Spring 2018

CONTENTS

Page

ABSTRACT

The “Husky One Card” is the name given to student IDs at the University of Connecticut. It can identify students, faculty, and staff in a variety of situations. The One Card is used for meal plans, Husky Bucks (an equivalent of money, but valid only in the Storrs area), residence hall/ university facility access, and student health services. The current Husky One Card consists of a picture identification on the front and a standard 1-dimensional barcode and 3-track magnetic strip on the back.

The goal of this thesis is to investigate the feasibility of cloning Husky One Cards, the ease with which one can obtain arbitrary student ID information, the robustness of the One Card backend system, and the risks posed by vulnerabilities. Cloning cards is first attempted with a fully-fledged magnetic strip read/writer and then with cheap, readily-available circuitry. Obtaining student ID information is carried out via a social engineering attack. Alternatively—and less trivially—student ID information may be inferred if attributes such as student name, graduation year, and major are known. Included is an analysis of how one may approximate student ID information based on this metadata. The One Card backend system is tested for effectiveness of “red flags,” which are meant to signal when a duplicate card is in use. Potential security enhancements to both the card itself and backend system are suggested at the end of this document. These recommendations account for usability, cost, and deployability.

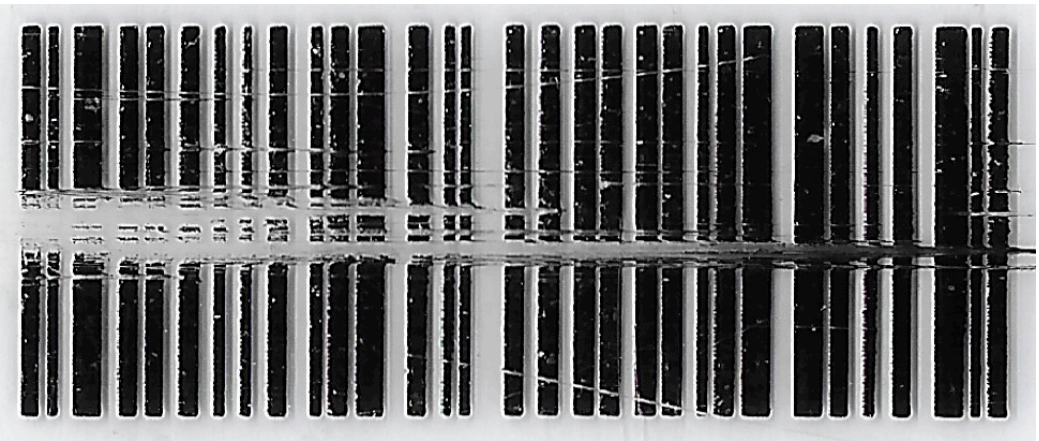
RULES OF ENGAGEMENT

Because this document deals with confidential student ID information and sensitive resources at the University of Connecticut, certain rules were followed and agreed upon by all involved parties to avoid jeopardizing the safety of students or the University. The involved parties consist of Trevor Phillips (author), Benjamin Fuller (thesis advisor), and Stephanie Kernozicky (Husky One Card Director). All parties agree that this task is limited to the ID cards of the involved individuals and dummy card accounts provided by the Husky One Card Office. However, these cards may be used in university systems after cloning to check efficacy. The author agrees not to clone a card of any UConn member without prior express consent from that member and from the Husky One Card Office. At no point should this thesis release student data or use card data in a scope outside of the study. Furthermore, the social engineering study has been approved by the University of Connecticut Institutional Review Board (IRB).

Details of cloning Husky One Cards may create financial risks to UConn and safety risks to One Card holders. All parties agree it is possible to produce a meaningful thesis without providing specific instructions of how to clone cards or revealing specific weaknesses in the underlying systems. Therefore the thesis has been released in two versions: one *public* version which omits the specifics of system vulnerabilities and details on how information is stored on Husky One cards; and one *private* version which includes full content (for use by University of Connecticut officials). The ■ symbol marks redacted content in the *public* version.

BACKGROUND

To understand what vulnerabilities may exist with the Husky One Card, one must first understand how the existing components work—i.e. the barcode and the magnetic strip. Shown below is a barcode scanned from a sample student ID.



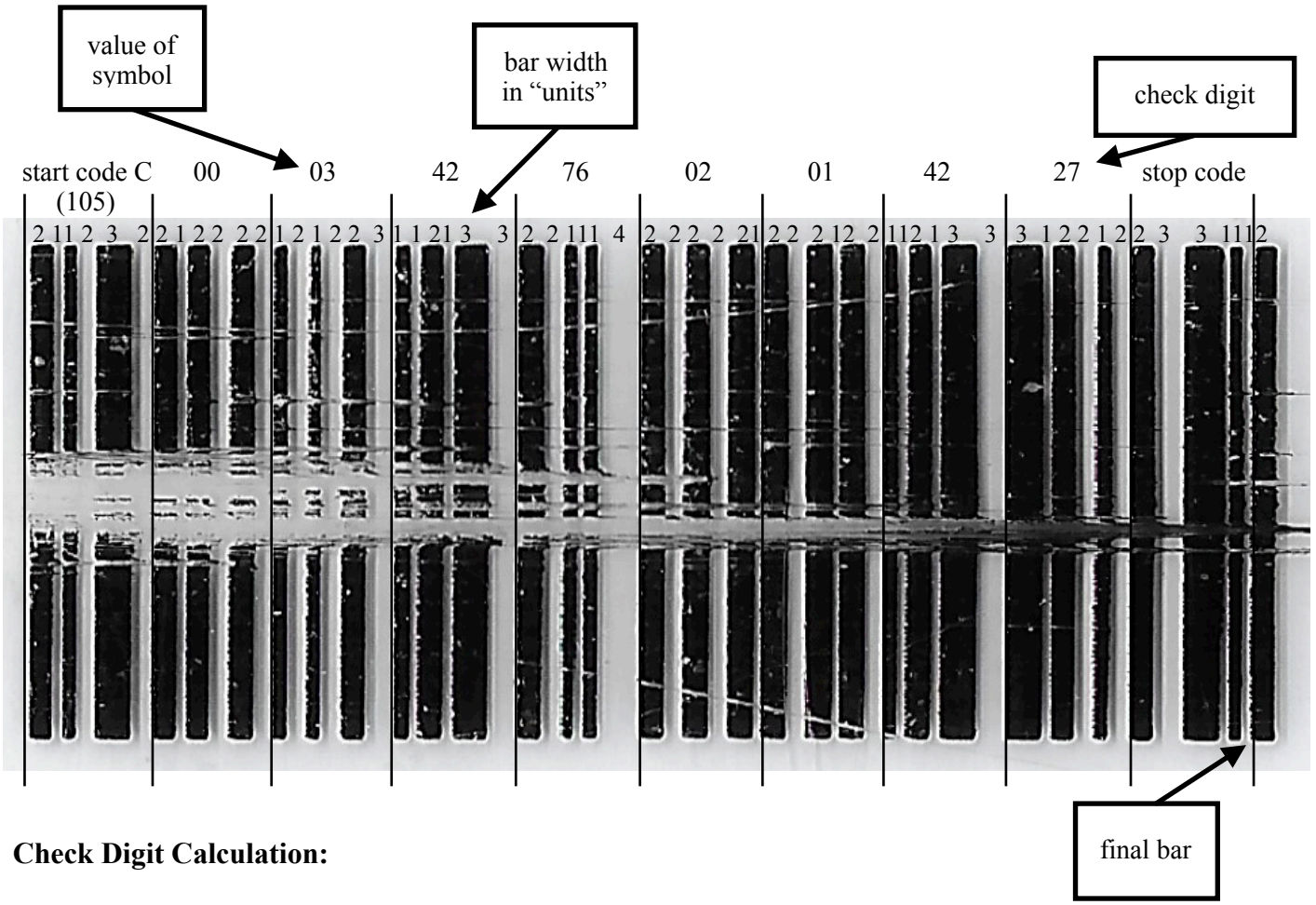
Barcodes can follow many encoding schemes. Universal Product Code (*UPC*) and European Article Number (*EAN*) encodings are commonly used for food and discount store items. The International Standard Book Number (*ISBN*) identifies books. "*Interleaved 2 of 5*" encoding is used for film and some products. The Husky One Card uses a somewhat newer encoding called "*Code 128,*" which provides a mapping for the entire ASCII character set. This type of barcode consists of 7 sections in the following order (Drollinger, Jennings and Stewart):

quiet zone → start code → data → check symbol → stop code → "final bar" → quiet zone

The start code, ASCII data symbols, and stop code are each encoded by three black bars and three spaces of various widths. The widths are between 1 and 4 "units" (the width of the "unit" is arbitrary and relative to the size of the barcode). For each symbol, the sum of the widths of the bars must be *even* whereas the sum of the widths of the spaces must be *odd*. Additionally, the total sum of "units" for a symbol must equal 11. *Code 128* shifts between three code sets—A, B, and C—where A and B encode ASCII characters and C encodes two-digit numbers. The Husky One Card uses *Code 128C*, meaning it encodes numbers only. The start symbol reveals which code set is used. For code set C, the start symbol value is 105 (2-unit bar, 1-unit space, 1-unit bar, 2-unit space, 3-unit bar, 2-unit space). A table of conversions which maps bar/space patterns to symbol values is publicly available on the Internet (Online, 2018).

A check symbol follows the data section and is calculated from a weighted sum of the start code value plus data symbol values, modulo 103 (Drollinger, Jennings and Stewart). The start code and first data symbol are weighted 1, and the weights of subsequent data symbols increase by 1 from there. See **Figure 1** for an example of checksum calculation and for the full breakdown of a *Code 128C* barcode on a sample Husky One Card.

Figure 1



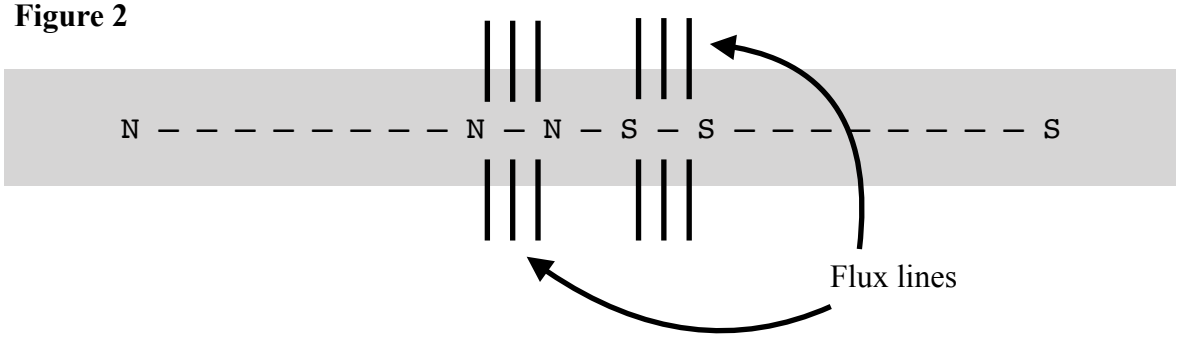
Check Digit Calculation:

Value	105	00	03	42	76	02	01	42	|	27
Weight	1	1	2	3	4	5	6	7		

(1)(105) + (1)(00) + (2)(03) + (3)(42) + (4)(76) + (5)(02) + (6)(01) + (7)(42) = 851
851 mod 103 = 27 ✓

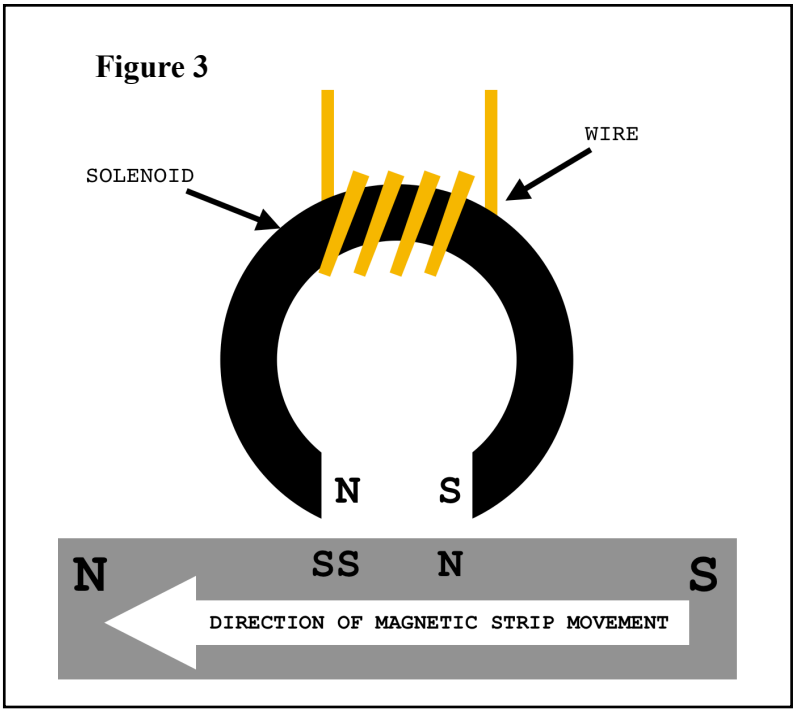
Magnetic strips, or *magstripes*, are slightly more complex because they involve electromagnetic forces. Magstripes contain tiny *ferromagnetic* particles which encode data. A ferromagnetic substance retains its magnetic polarity after an external magnetic field is removed. On a blank magstripe, all particles are aligned with adjacent north-south poles such that one end of the strip is the overall "north pole" and the other end the "south pole." If a section of the strip is exposed to a strong enough magnetic field with the opposite polarity, that section's particles will themselves flip, causing a break in the adjacent north-south chaining of particles. Such a break creates *flux lines* in the electromagnetic field (*flux* being an electromagnetic "flow" perpendicular to the card surface). See **Figure 2**.

Figure 2



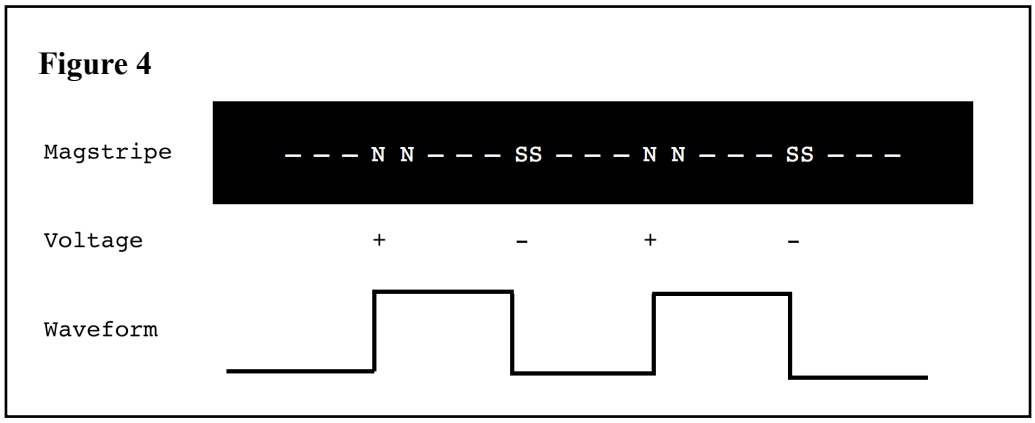
Polarities in sections of the magstripe can be flipped by a solenoid. A solenoid designed to encode magstripes is shown in **Figure 3**. Current flows through a wire wrapped around a metal ring. On the ring, magnetic north and south poles are forced close together across a small gap. This creates a strong magnetic field in the gap. When the magstripe moves near this gap and the current flowing through the wire is *reversed*, the section of the magstripe exposed to the gap will polarize to the *opposite* of the gap's polarity. Thus data on an encoded magstripe is represented by a series of flux reversals.

Figure 3



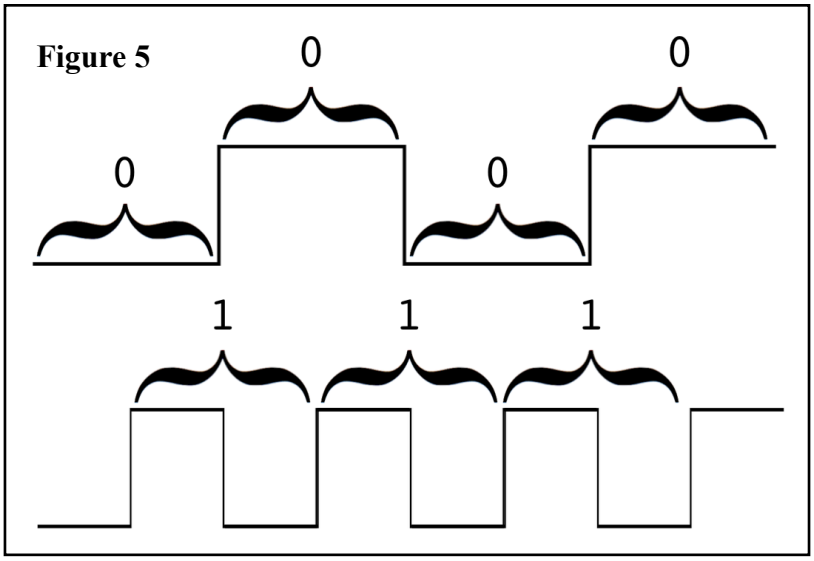
Using current to generate a flux reversal describes a technique for *writing* to a card. The method of *reading* from a card works in the opposite manner. When a magnetic field passes through the gap of a solenoid such as in **Figure 3**, it produces a current in the coil. Using this phenomenon, magstripe readers can determine where flux reversals occur and translate them into voltage peaks and troughs. **Figure 4** shows these voltage peaks and troughs as a square waveform. “NN” reversals correspond to positive voltages and “SS” reversals correspond to negative voltages (Count Zero, 1992).

Figure 4



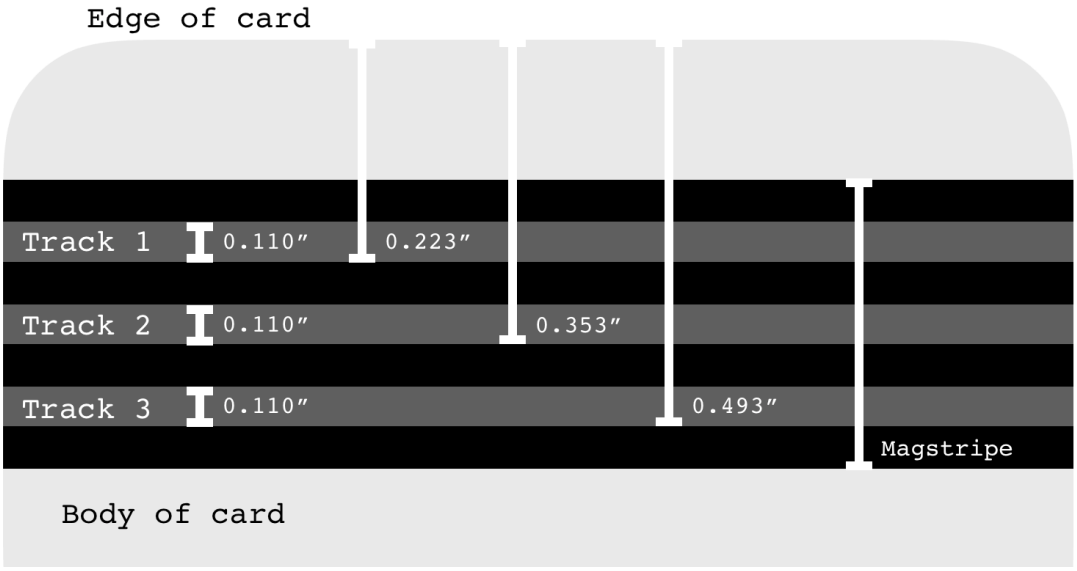
The square waveform can be converted to binary card data. However, high and low points in the waveform *do not* correspond to 1s and 0s of the binary data. Instead, because cards may be swiped at different speeds, a method known as *Differential Manchester encoding* is used to form a self-synchronizing data stream. In other words, it is the *frequency* of the waveform which encodes data. The frequency of the “1” signal is always twice that of the “0” symbol on the waveform. For an example, see **Figure 5**.

Figure 5



The binary data on magstripes typically uses *BCD* encoding format ("Binary Coded Decimal") or *ALPHA* format. *BCD* format uses 5 bits per symbol and encodes numbers. *ALPHA* format uses 7 bits and encodes numbers, letters, and special symbols. The encoding protocol varies on each *track* of the magstripe. Standard magstripes have three tracks, shown in **Figure 6** (Count Zero, 1992).

Figure 6



On a standard magstripe, Track 1 uses *ALPHA* format whereas Tracks 2 and 3 use *BCD* format. This is important because different "sentinel" symbols are used on each track, depending on the data format.

Track 1	Track 2	Track 3
Start sentinel: % Field separator: ^ End sentinel: ?	Start sentinel: ; Field separator: = End sentinel: ?	Almost never used

Each track begins with a series of all-zero bits called *clocking bits* which are used by the card reader to self-synchronize. The overall layout of a typical magstripe track is shown below:

clocking bits → start sentinel → data → field separator → data → end sentinel → clocking bits

METHODOLOGY

The investigation of the security of Husky One Cards can be broken into various segments of interest. A preliminary analysis of the technologies and encoding scheme used by the One Card offers a starting point for further investigation. From there, card duplicating methods are explored. To assess the ease with which one can obtain arbitrary ID information, a social engineering experiment was conducted. Finally, the overall One Card system was tested by circulating duplicated cards in common usage situations.

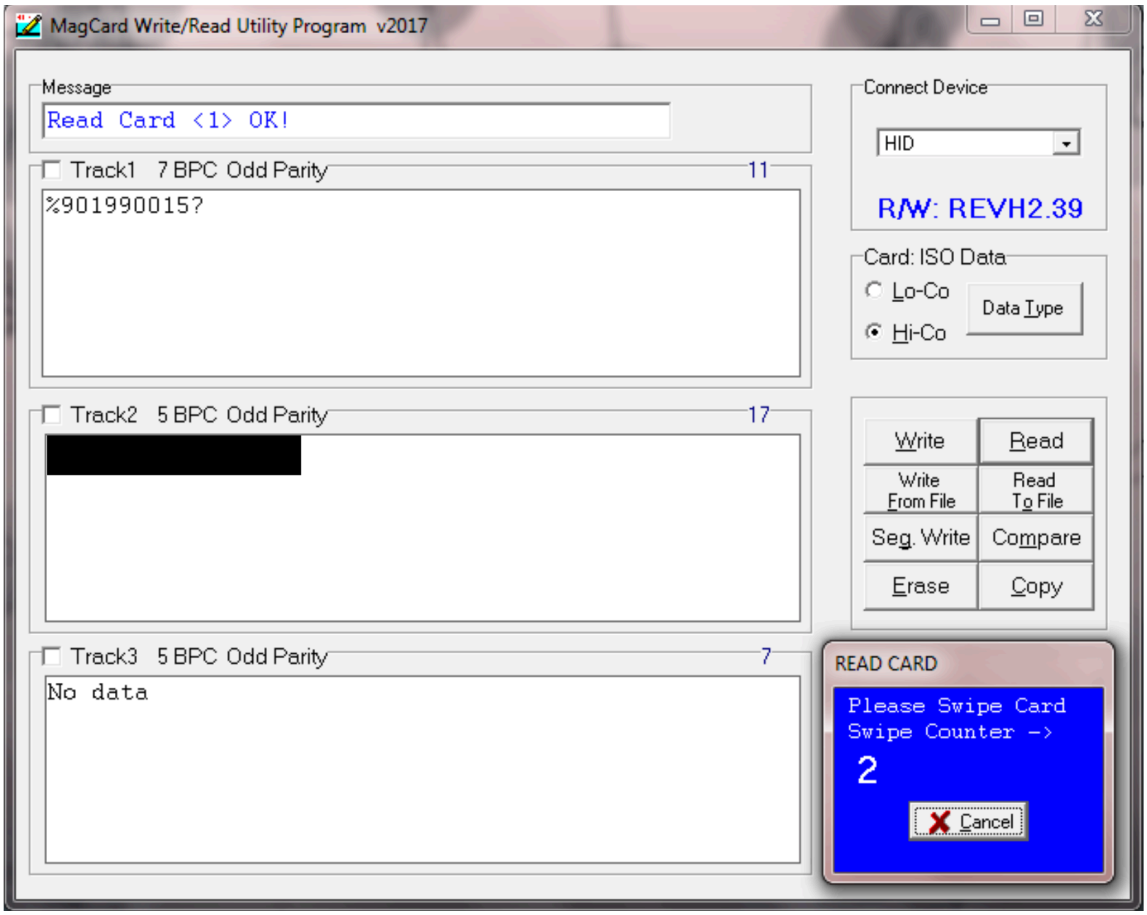
Preliminary Analysis

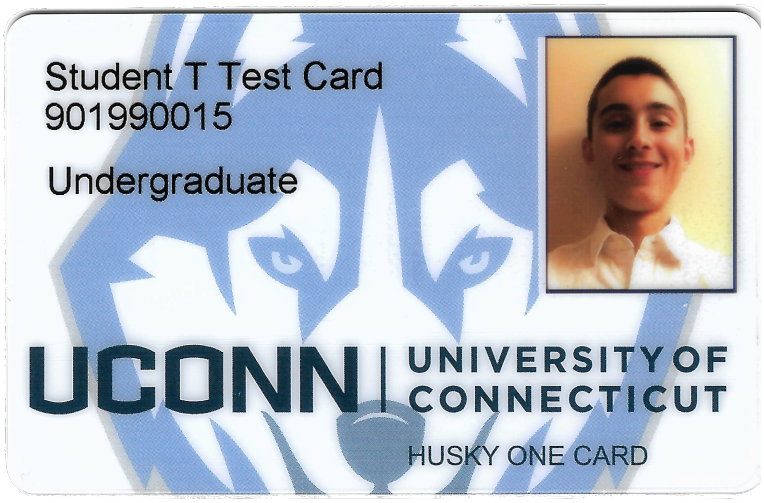
As mentioned in the **Background**, the Husky One Card barcode uses a *Code 128C* encoding and has seven data symbols, all of which are two-digit numbers. A simple $15 card reader purchased online was used to determine the contents of a sample card's magstripe. On the strip, only tracks 1 and 2 contain data. The data on track 1 (*ALPHA* format) is simply ■■■. The data on track 2 is more interesting and is *equivalent to* ■■■. Specifically, track 2 contains 14 digits with a field separator after the first 10 digits. For example, track 2 data may look something like `;`■■■=■■■`?` where `;` is the start sentinel, = is the field separator, and `?` is the end sentinel. Because track 2 is equivalent to ■■■, it is possible that this is the "relevant" data used by the backend card system to validate an ID. If one understands how the University of Connecticut creates data for track 2, it represents a serious risk to the University. A malicious attacker could generate this data without cloning an existing card if he or she grasps how the underlying system works. Additionally, if the range of values for track 2 is limited (e.g. if most digits are the same across different cards), a brute force attack could prove successful. In other words, the attacker could pick random values for the unpredictable digits and still produce a working card. A more in-depth analysis of card data patterns is given in the **Social Engineering** section.

Card Cloning Machine

Card read/writing equipment can be obtained for less than $100 from most online retailers. For this thesis, the *OSAYDE Model 605U* reader/writer was purchased for $85, including 20 blank magstripe cards. The *605U* can read and write all three tracks on a magstripe and functions with both high and low coercivity cards. The card reader works with Windows software pictured in **Figure 7**, allowing users to easily read/write/erase data onto any card. A test ID provided by the Husky One Card Office proved easy to duplicate with this technology. Emulating the face of the card was also simple: scan the real card, then print copies to scale and cut them out. Apply glossy tape to simulate the feel of the smooth, reflective finish on genuine student IDs.

Figure 7





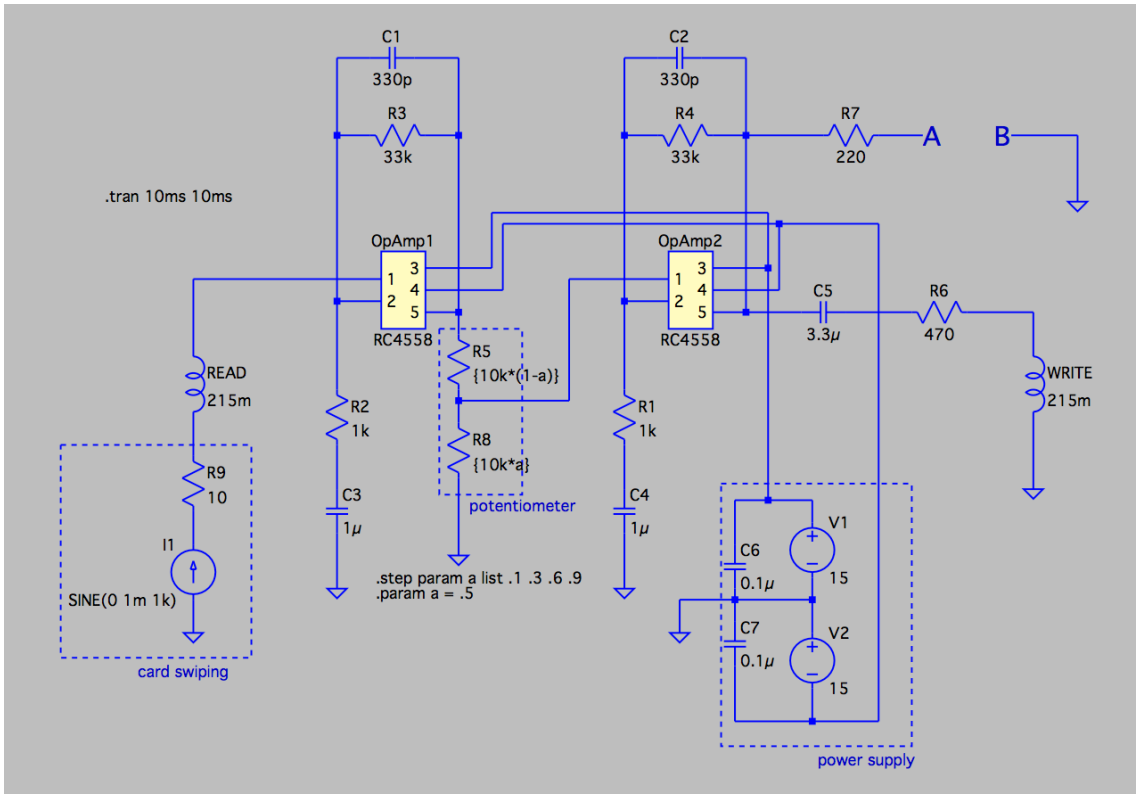
Test ID provided by the Husky One Card Office

Working, duplicated IDs (middle ID is real)

Card Cloning Circuit

ID cards can be duplicated quite easily using commercially available card writers, however this thesis aims to find out whether cheap, readily-available circuitry can also be used to create a card-cloning mechanism. **Figure 8** shows a circuit modeled in LTSpice which can provide card-duplicating functionality (Count Zero, 1992). The read- and write-heads are modeled as 215mH inductors and the signal generated by a card swipe is modeled as a 1mA sinusoidal waveform. Because the signal from the card swipe is small and the write-head requires a large signal to write HiCo cards, two 4558 op amps are used to amplify the input signal. The actual read- and write-heads were produced by Global Manufacturing Industries; the read-head is part #H816148 and the write head is part #H814080. Schematics for these parts are provided on pages 13-14.

Figure 8

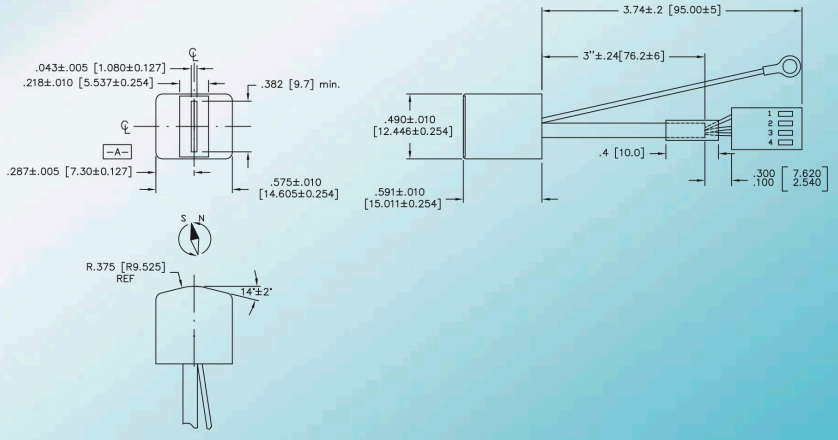


In practice, the read- and write-heads are positioned in series and two cards, one with data and one that is blank, are swiped at the same time. The encoded card is placed over the read-head and the blank card is placed over the write-head. The circuit picks up the signal from the read-head and instantaneously transfers it to the write-head, which then encodes data onto the blank card. **Figure 9** shows the physical setup. It is worth noting that the parts used for this circuit can be purchased for a few cents to a few dollars apiece.

Magstripe Read Head - Global Manufacturing Industries Part No. H816148

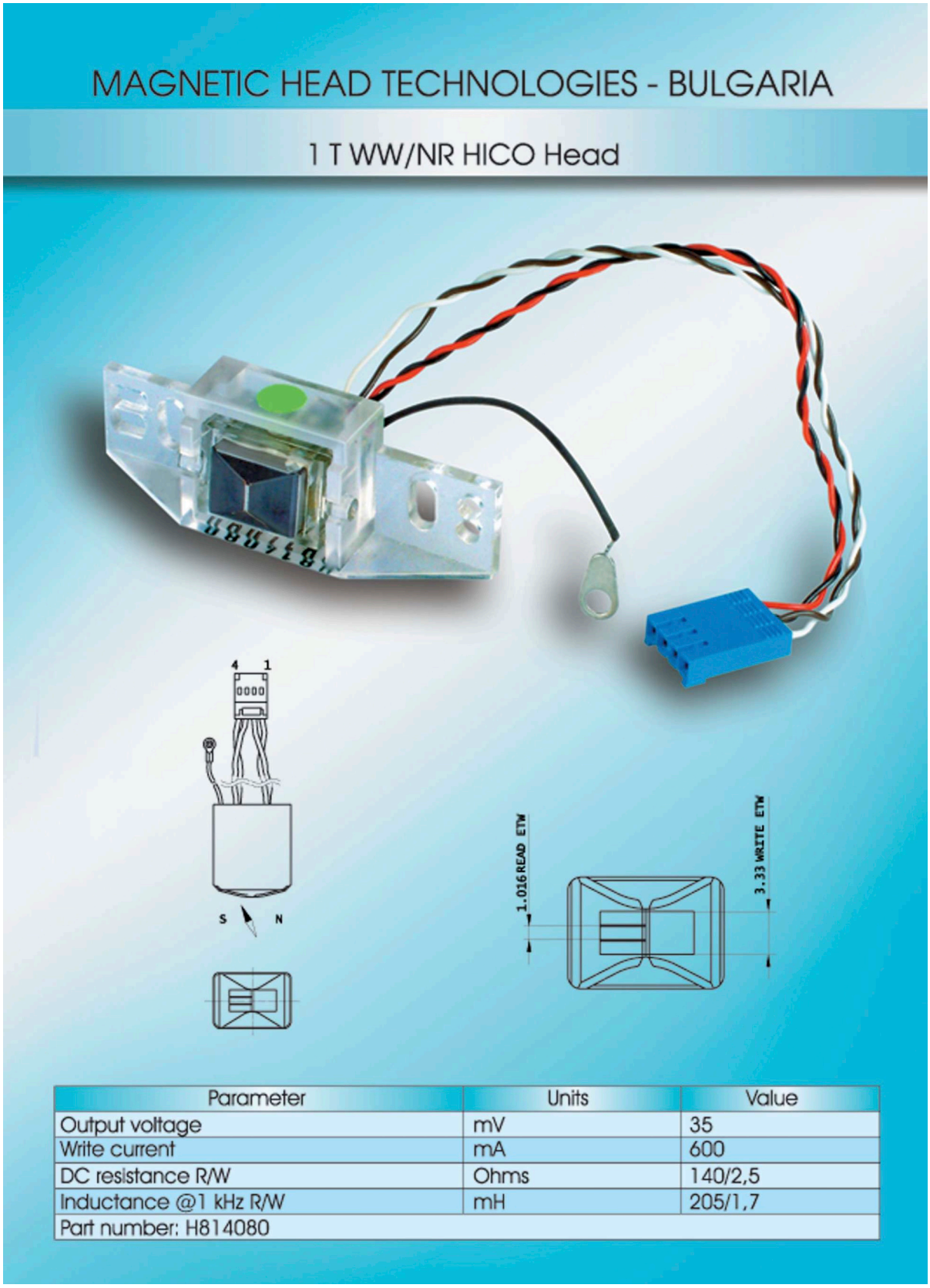
MAGNETIC HEAD TECHNOLOGIES – BULGARIA

1 CH. READ HEAD



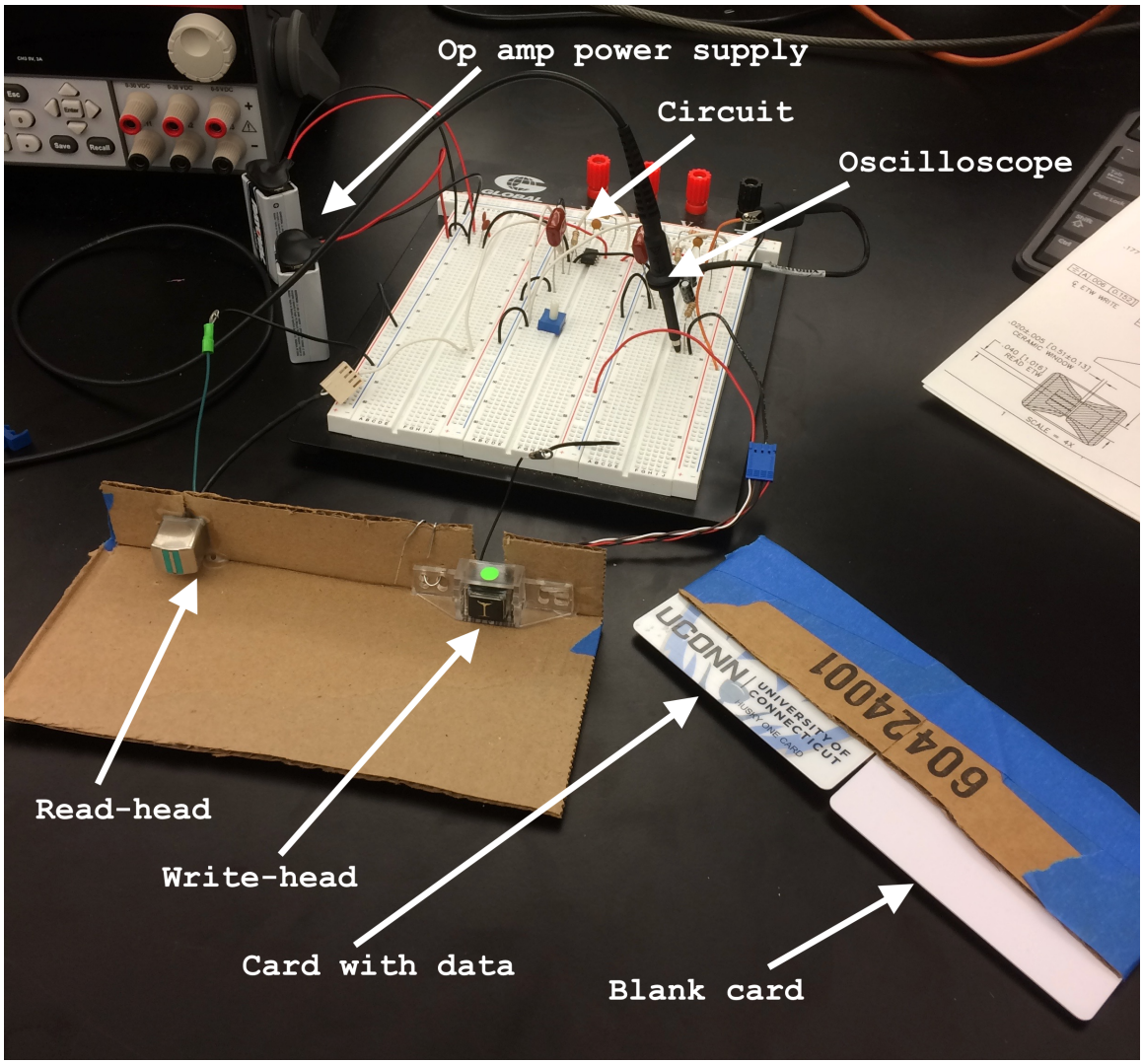
Parameter	Units	Value
D. C. Resistance	Ohms	200
Inductance @ 1 kHz	mH	215
Read Output	mV	105
Part number: H816148		

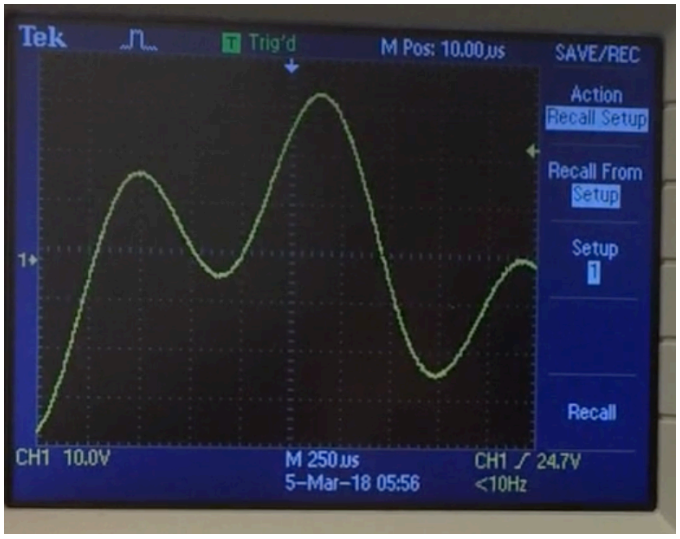
Magstripe Write Head - Global Manufacturing Industries Part No. H814080



Parameter	Units	Value
Output voltage	mV	35
Write current	mA	600
DC resistance R/W	Ohms	140/2,5
Inductance @1 kHz R/W	mH	205/1,7
Part number: H814080		

Figure 9





Pictured above, the card-duplicating circuit.

On the left, a sample of the signal generated by swiping a UConn Husky One Card after amplification by two operational amplifiers.

The functionality of the read- and write-heads used for the card duplicating circuit is limited, as they can only read and write one track at a time. In addition, the heads require extremely precise horizontal and vertical alignment of the cards to make an accurate read/write. Because of this, a fully-working duplicated ID was not achieved with the setup of **Figure 9**, however a working card cloner is highly possible if the makeshift cardboard construction is abandoned and a more exact framework is used to align the cards with the magnetic heads. Moreover, the circuit described here is not the only method of falsifying IDs. Other methods have also proved successful such as the custom hardware/software solution developed by students at the University of Maryland (Ramsbrock and Moskovchenko).

Social Engineering

To determine the ease with which an attacker could obtain a student's ID information, a social engineering experiment was conducted after approval from the University of Connecticut Institutional Review Board (study H19-009). For five hours, researchers manned a table in the Student Union, a highly frequented location at the University of Connecticut. Undergraduate students over the age of 18 who passed by were asked if they would be willing to participate in a research study to help improve the security of the UConn campus. If the students consented, they would be asked to swipe their ID and fill out a brief questionnaire. Students were then informed of the true purpose of the study and could request to have their data removed from the study results. Over a five hour period, 22 subjects participated and consented for their results to be used anonymously in card data analysis.

Results from the social engineering study indicate that there *are* underlying patterns in the data encoded on Husky One Cards. The data on track 1 is ■■■. Track 2 contains 14 digits with a field separator after the first 10 digits. Track 3 is blank. The table below summarizes experimental findings relevant to track 2 data:

Digit Position	1-3	4	5-9	10	11	12	13	14
Range of Values	■	■	■	■	■	■	■	■
Meaning	*counter*			?	*issue code*	?		

Counter: Based on the results of the study, we can make a reasonable guess as to the meaning behind the digits in track 2. A questionnaire was used to gather each research participant's NetID, PeopleSoft number, birth date, and admission date at UConn. When respondents are ordered based on their admission date, the number formed by digits 1-9 in track 2 *increases*. For example, the nine-digit number formed by positions 1-9 in track 2 is *smaller* for all students who were admitted to UConn in Fall 2014 compared to those who were admitted in Fall 2015 or 2016. From this observation, it is reasonable to assume that digits 1-9 represent a simple counter which increases for each new student enrolled at UConn. To further support this argument, the most-significants positions in the nine-digit counter should change the least, which

was an observed pattern in the results. ■■■. Digit 4 changed least frequently among digits 4-9. From the 22 responses, digit 4 was oftentimes ■■■; in only one case was it equal to ■■■. The number formed from digits 1-9 using the test ID for this thesis is equal to ■■■— a high number likely chosen because the student ID "counter" will not reach this level in the near future.

Issue code: The issue code begins at 0 when a student is first given his or her ID. If a student loses his or her ID and is issued a new one, this number is incremented by one. The issue code was 0 or 1 for the majority of students, so we will assume the issue code is 0 or 1 for subsequent analysis. The meaning of this digit was determined by asking students how many times they had been issued a replacement ID during the experiment.

Other digits: Digits 10, 12, 13, and 14 were the same among all IDs swiped, thus it is difficult to determine the meaning behind these digits. They could simply be arbitrary constants for all Husky One Cards, or perhaps there is variation between undergraduate students, graduate students, faculty, and staff.

We can estimate the potential combinations of track 2 data as follows:

$$1^3 \cdot 3 \cdot 10^5 \cdot 1 \cdot 2 \cdot 1 \cdot 1 \cdot 1 = 600{,}000$$

The probability of even one brute force attempt being valid is given below—about 6%. In other words, choosing random values for unpredictable digits results in a 6% likelihood of producing a working card. However, the odds of a correct guess significantly increase if the attacker knows the target's admission date and how many times he or she has been issued a replacement ID. If the backend system validates only a portion of the data on each card, there is additional margin for error on the attacker's part, again increasing the likelihood of a successful randomized, brute force attack. Note that 32,027 represents the total student enrollment for UConn in Fall 2016 and 4,830 represents the total full-time and part-time faculty and staff for Fall 2016 (University of Connecticut, 2017). It is assumed that the entire UConn population has a valid Husky One Card with unique track 2 data.

$$\frac{\textit{UConn population}}{\textit{track 2 combinations}} = \frac{32{,}027 + 4{,}830}{600{,}000} = 6.1\%$$

Card System Backend

Two tests were conducted to analyze the efficacy of the Husky One Card backend system. Both tests involved swiping multiple copies of the same ID within a narrow time window at various locations around the University of Connecticut campus. The card used for testing was a sample ID provided by the Husky One Card Office.

Test 1 - 2/21/18 at approximately 4:50 pm

Locations: (1) Husky Village B2 residence hall, (2) Towers dining hall
Time window: 10 seconds
Result: The backend system *did not* detect any abnormal activity

Test 2 - 2/23/18 at approximately 12:15 pm

Locations: (1) Towers dining hall, (2) McMahon dining hall, (3) South dining hall
Time window: 2 minutes
Result: The backend system *did* detect abnormal activity

The backend card system used by the University of Connecticut to manage the One Card is know as CBORD (CBORD) and interestingly, it only detected one of the two tests. This is likely because the second test was performed at only one type of entry point—dining facilities—whereas the first test utilized two entry points—residence halls and dining facilities. These results suggest that the backend system is not fully integrated across entry points, which can be wide-ranging: dining halls, residence halls, campus cafés, student events, vending machines, and even local businesses which accept the One Card as a form of payment. Such a finding leads to serious concerns about the ability to detect duplicate IDs. An unethically replicated card could be used to gain access to a dormitory and to make a purchase at the same time. If the backend system does not perform a holistic analysis of card usage, the probability of detection is greatly reduced. In other words, malicious users would have to perform a synchronized swipe at a single type of entry point for the system to have a chance of raising a red flag.

Furthermore, it is worth considering the human element when analyzing these tests. Swiping into a dining hall at the University of Connecticut involves handing an ID to a worker at the entrance, who then swipes the ID and verifies the photo on the card. During the second test, two of the three IDs used to swipe into dining halls were *completely blank*, containing only data encoded on their magstripes. However, for both blank cards in the second test, entry into the dining facilities was granted. Although the workers found the cards unusual in appearance, they allowed entry with little to no questioning. This finding raises further concerns about the possibility of widespread circulation of duplicate student IDs.

RISK ASSESSMENT

The various methods of attacking the Husky One Card system present a serious risk to the University and its student population. For $1000-$2000, an attacker could purchase a fully-functioning card maker with the ability to print graphics onto cards. For less than $100, an attacker could acquire a magstripe-writer such as the *OSAYDE Model 605U* and could encode arbitrary data onto ID cards. Perhaps the most concerning is this machine's capability to overwrite existing HiCo card data. For example, an attacker possessing his own student ID could encode *someone else's* information onto his magnetic strip. Finally, for less than $20, an attacker could construct a "homemade" card cloning machine, although this requires more familiarity with electronic circuit design.

Not to be overlooked are the vulnerabilities in the card system backend and the inherent naiveté of students and staff concerning their IDs. The failure of the CBORD system in one of the two tests suggests that a change should be made to more effectively detect use of duplicate IDs. The dining facility employees' willingness to admit students who supplied completely blank Husky One Cards with no photo identification should provide additional evidence that a change is in order. Lastly, if the social engineering experiment was carried out by a malicious attacker, the private data of 22 students could have been compromised after a single day. Results from this experiment demonstrate that students tend to be unaware of the ease with which their card data can be stolen. With a student's card data in hand, an attacker could take advantage of the student's meal plan and "Husky Bucks." More troubling however, the attacker could also gain access to the student's residence hall and dormitory. Although individual dormitories in residence halls have a second layer of security—a physical lock with a corresponding key issued to each resident—many students leave their rooms unlocked throughout the day. In addition, the same social engineering attack carried out on faculty and staff could have much greater implications; the attacker could potentially gain access to restricted areas around campus and jeopardize the physical safety of students.

COUNTERMEASURES

This section details actions which may be taken to mitigate the risks of the current One Card system and potential improvements to the system. Factors such as usability, cost, and deployability are also taken under consideration. For the subsequent discussion, we will use the following assumptions and estimations given by University of Connecticut officials:

- The average cost of manufacturing a student ID for the University is about ■■■
- There are approximately 17,800 student IDs issued per year
- The typical cost of a card reader varies by model, but estimates are shown below:

Name	Number in use	Average cost per unit	Total cost
■	16	$150	$2,400
■	3	$6,000	$18,000
■	14	$100	$1,400
■	15	$400	$6,000
■	28	$800	$22,400
■	2	$1,800	$3,600
■	29	$1,000	$29,000
■	2	$2,000	$4,000
■	124	$300	$37,200
Total	233	**Total**	$124,000

From this data, the average cost of a card reader to the University of Connecticut is $532.19.

Countermeasure 1: Train staff members to examine Husky One Cards for forgery. Perhaps the cheapest and most effective method for detecting misuse of a student ID is for personnel swiping the card to compare the headshot on the card to the individual who is using it, and to inspect the card for obvious signs of forgery. This countermeasure requires no additional technology and incurs little cost to the University. The only foreseeable cost is that of training staff to place increased emphasis on comparing ID to user. However, in practice this method has serious drawbacks and limited potential. In situations where card access is automated (such as entering dormitories and automatic check-outs) personnel cannot guard against fake IDs. In addition, staff members are often faced with a rush of students at peak hours of the day. In these situations, with a queue building up, staff members may feel pressure to swipe IDs as quickly as possible and will pay little regard to examining cards for forgery.

Countermeasure 2: Implement two-factor authentication with a PIN. Additional security in the form of a "*Personal Identification Number*" (PIN) offers a simple yet effective mechanism for preventing identity theft. This solution requires that, after swiping his or her ID, a student must also input his or her PIN into a keypad. Deployment requires the following actions: pairing keypads with card reader devices, modifying the backend system to track PIN numbers along with ID information, updating the Husky One Card website to allow cardholders to update PINs and recover forgotten PINs, and training staff on usage of the new system. While the cost of implementing these changes may be larger than that of the first countermeasure, the additional security gained by making these changes may be worth the fee. Using a PIN may also slow down the movement of lines at dining facilities and checkout counters, however instituting a PIN at automated access points only (such as residence halls) may offer a compromise.

Countermeasure 3: Adopt RFID technology. Deployment of passive RFID tags onto Husky One Cards is cheaper than using active or semi-passive tags but just as effective for this use case; most passive RFID tags cost between 7 and 20 cents each (Bonsor and Fenlon, 2007). This strategy makes use of "*Near Field Communication*" (NFC), a system gaining rapid popularity with credit and debit card companies. With NFC, the user of a One Card taps his or her card against NFC payment terminals instead of swiping, thereby eliminating the possibility that an attacker could skim the user's data via the magnetic strip.

The passive tag mechanism work as follows (Bonsor and Fenlon, 2007):

1. The tag microchip is encoded with data (potentially up to 2 kilobytes)
2. The tag antenna receives electromagnetic energy from an RFID reader antenna
3. The chip sends radio waves to the reader using power from the reader's electromagnetic field
4. The RFID reader parses the tag's radio waves into data

It is worth noting that there are vulnerabilities and drawbacks that arise from using RFID technology. An attacker could execute a s*kimming* attack by using an RFID reader to scan data from an RFID chip without the card holder's knowledge. *Eavesdropping* presents another vulnerability, if an attacker were to read the frequencies emitted from an RFID chip as it is scanned by an official reader. Disturbingly, passive tags can be read from up to 20 feet away (Bonsor and Fenlon, 2007). RFID chips present a more secure option than outdated magstripes only if the RFID data is encrypted and the chip uses a rolling code. Some RFID chips can be read from and written to multiple times. A rolling code means that after every transaction, a new code is written to the chip and this code is tracked by the backend system. Then, even if an attacker skims a user's card, the skimmed data will be invalid if the card holder uses his or her card before the attacker is able to create and use a duplicate.

For a discussion of the cost of implementing an RFID card system, a representative from IdentiSys, Inc.—a full-service identification and security solutions provider—furnished the following quote:

Item	Quantity	Average cost per unit	Total cost
Proximity card, standard HID format (26-bit) with magstripe *	1,800	$2	$3,600
SD360 Dual-Sided ID Badge Printer with magstripe encoder	1	$1,800	$1,800
Color ribbon, YMCKT-KT **	6	$140	$840
ID badging software	1	$250	$250
** yearly cost, ** assuming 300 cards per ribbon*		**Total**	$6,490

CONCLUSION

After a comprehensive analysis of the University of Connecticut Husky One Card system, a surprising number of flaws and vulnerabilities were found. A test ID provided by the One Card Office was duplicated and used in a variety of situations, and the cards of 22 undergraduate students could have been cloned just as easily by a malicious individual. Humans may always be susceptible to social engineering attacks, but the technology used for access control and payment at the University deserves an upgrade. Magnetic strip technology is largely outdated at present. Banks, hotels, and other businesses which issue cards are moving towards RFID chips, two-factor authentication, and biometrics. The University will of course incur a cost when upgrading to one of these technologies, but officials must weigh this cost against the improved security afforded to UConn students, faculty, and staff.

ACKNOWLEDGEMENTS

I would like to thank Dr. Benjamin Fuller for being the primary advisor of this thesis. His assistance in working with the Institutional Review Board to approve the social engineering experiment was enormously helpful, as was his support in the delicate matter of obtaining approval from the University of Connecticut to clone cards and publicizing information regarding the campus ID system. I would also like to thank Stephanie Kernozicky, Director of the One Card Office, for her invaluable assistance in providing a working “dummy” student ID and serving as a reference for inquiries about the UConn ID system. Finally I would like to thank Jim Tusing from Global Manufacturing Industries for shipping read- and write-heads all the way from Bulgaria at no charge, and for answering many of my questions about the operation of these magnetic heads in a circuit.

REFERENCES

Bonsor, K. & Fenlon, W., 2007. How RFID Works. HowStuffWorks. Available at: https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/rfid.htm [Accessed April 10, 2018].

CBORD, Powered by CBORD. The CBORD Group. Available at: https://cbord.com/ [Accessed April 10, 2018].

Count Zero, 1992. Card-O-Rama: Magnetic Stripe Technology and Beyond. gae.ucm.es. Available at: http://www.gae.ucm.es/~padilla/extrawork/card-o-rama.txt [Accessed April 10, 2018].

Drollinger, R., Jennings, M. & Stewart, R., Bar code Encoding of Strings. washington.edu. Available at: https://courses.cs.washington.edu/courses/cse370/01au/minirproject/theBarCoders/barcodes.html [Accessed April 10, 2018].

Online, 2018. Code 128. Wikipedia. Available at: https://en.wikipedia.org/wiki/Code_128 [Accessed April 10, 2018].

Ramsbrock, D., Moskovchenko, S. & Conroy, C., Magnetic Swipe Card System Security. umd.edu. Available at: https://www.cs.umd.edu/~jkatz/THESES/ramsbrock.pdf [Accessed April 10, 2018].

University of Connecticut, 2017. 2017 Fact Sheet. uconn.edu. Available at: https://uconn.edu/content/uploads/2017/01/INT-003-Fact-Sheet-011117-WEB-1.pdf [Accessed April 10, 2018].

APPENDIX: STUDY H19-009

UCONN
UNIVERSITY OF CONNECTICUT

DATE: March 30, 2018

TO: Benjamin Fuller, Ph.D.
Computer Science and Engineering

FROM: Pamela I. Erickson, Ph.D.
Chair, Institutional Review Board
FWA #00007125

RE: Protocol #: H18-009 "Improving Security of UConn"
Funding Source:
Approval Period: From: March 30, 2018 Valid Through: March 30, 2019
"Expiration Date"

On March 16, 2018, the Institutional Review Board (IRB) reviewed the above-referenced research study by expedited review and determined that modifications were required to secure approval. Those requirements have been met, and the IRB granted approval of the study on March 30, 2018. The research presents no more than minimal risk to human subjects and qualifies for expedited approval under category # 7 - Research on individual or group characteristics or behavior (including, but not limited to, research on perception, cognition, motivation, identity, language, communication, cultural beliefs or practices, and social behavior) or research employing survey, interview, oral history, focus group, program evaluation, human factors evaluation, or quality assurance methodologies.

Per 45 CFR 46.116(d), the IRB approved the consent procedure outlined in the protocol involving use of deception, thereby altering some elements of informed consent. The IRB finds and documents that (1) the research involves no more than minimal risk to the subjects; (2) the waiver or alteration will not adversely affect the rights and welfare of the subjects; (3) the research could not practicably be carried out without the waiver or alteration; and (4) whenever appropriate, the subjects will be provided with additional pertinent information after participation.

Enclosed is the validated consent form. **A copy of the approved, validated consent form (with the IRB's stamp) must be used to consent each subject.**

All investigators at the University of Connecticut are responsible for complying with the attached IRB "Responsibilities of Research Investigators."

Re-approval: It is the investigator's responsibility to apply for re-approval of ongoing research at **least once yearly**, or more often if specified by the IRB. The Re-approval/Completion Form (IRB-2) and other applicable re-approval materials must be submitted **one month** prior to the expiration date noted above.

Modifications: If you wish to change any aspect of this study, such as the procedures, the consent forms, the investigators, or funding source, please submit the changes in writing to the IRB using the Amendment Review Form (IRB-3). All modifications must be reviewed and approved by the IRB prior to initiation.

Audit: All protocols approved by the IRB may be audited by the Research Compliance Monitor.

Please keep this letter with your copy of the approved protocol.

Attachments:

1. Validated Consent Form
2. Validated Recruitment Material
3. Validated IRB-1 Application and Study Protocol Forms
4. "Responsibilities of Research Investigators"

Office of the Vice President for Research
Research Compliance Services
438 WHITNEY ROAD EXTENSION, UNIT 1246
STORRS, CT 06269-1246
phone 860.486.8802
fax 860.486.1044
compliance.uconn.edu

Consent Form for Participation in a Research Study

Principal Investigator: Benjamin Fuller
Student Researcher: Trevor Phillips
Study Title: Improving Security of UConn

Introduction

You are invited to participate in a research study to help improve the security of UConn. You are being asked to participate because you are a UConn undergraduate student with an active Husky OneCard.

Why is this study being done?

The purpose of this research study is to collect demographic information about UConn undergraduates and see if this information can be correlated with public data sets.

What are the study procedures? What will I be asked to do?

If you agree to take part in this study, we will first confirm that you are an undergraduate UConn student over the age of 18. Then, you will be asked to complete three actions: (1) swipe your student ID in a card reader, (2) fill out a brief online survey with information about your NetID, PeopleSoft number, school admission date, and birth date, and (3) have a photo taken of yourself.

The study will be conducted at a table in the Student Union, nearby the Student Union Game Room. The time to complete this study should take no more than 5 minutes of your time. You will not be contacted after the study. We will further explain the purpose of the study at the conclusion of the study.

What are the risks or inconveniences of the study?

There are minimal risks to completing this study.

- Parts 1 (swiping your student ID), 2 (taking the survey), and 3 (taking a photo) all have minimal risks. The collected data will be stored on an encrypted UConn computer that is only accessible through secure protocols. The main risk is that someone breaches this computer and compromises this information. The information will be purged upon completion of the required analysis. Additionally, all data will be completed no more than 3 years after your engagement in the protocol. Photographs will be destroyed immediately after completing of the study.

The steps taken to minimize these risks are as follows: your student ID information and survey results will be stored securely in a locked location by Dr. Fuller, on a UConn computer. Your student ID information and survey results will not be publicized.
We expect the study to take between 2-5 minutes of your time to complete.

What are the benefits of the study?

You may not directly benefit from this research; however, we hope that your participation in the study may, in the long run, improve security of the UConn community.

Will I receive payment for participation? Are there costs to participate?

There are no costs and you will not be paid to be in this study.

How will my personal information be protected?

The following procedures will be used to protect the confidentiality of your data. The researchers will keep all study records (including any codes to your data) locked in a secure location. Your survey data will be hosted on the UConn Qualtrics survey website and then data will be transferred to a secure computer in Dr. Benjamin Fuller's office. The data taken from your student ID. The data will be stored no longer than 3 years and will be deleted upon completion of analysis.

All electronic files (e.g., database, spreadsheet, etc.) containing identifiable information will be password protected and stored on an encrypted computer. Any computer hosting such files will also have password protection to prevent access by unauthorized users. Only the members of the research staff will have access to the passwords. At the conclusion of this study, the researchers may publish their findings. Information will be presented in summary format and you will not be identified in any publications or presentations.

We will do our best to protect the confidentiality of the information we gather from you but we cannot guarantee 100% confidentiality. Your confidentiality will be maintained to the degree permitted by the technology used. Specifically, no guarantees can be made regarding the interception of data sent via the Internet by any third parties.

Study data may be released, but no information that allows others to identify you will be released. Data that may be released will be aggregate statistics about the results of the study, such as how many people participated. Your name will not be released.

You should also know that the UConn Institutional Review Board (IRB) and Research Compliance Services may inspect study records as part of its auditing program, but these reviews will only focus on the researchers and not on your responses or involvement. The IRB is a group of people who review research studies to protect the rights and welfare of research participants.

Can I stop being in the study and what are my rights?

You do not have to be in this study if you do not want to. If you agree to be in the study, but later change your mind, you may drop out at any time. There are no penalties or consequences of any kind if you decide that you do not want to participate. In addition, you do not have to answer any question that you do not want to answer.

Whom do I contact if I have questions about the study?

Take as long as you like before you make a decision. We are happy to answer any question you have about this study. If you have further questions about this study or if you have a research-related problem, you may contact the principal investigator, Dr. Benjamin Fuller at benjamin.fuller@uconn.edu, or the student researcher Trevor Phillips at trevor.j.phillips@uconn.edu. If you have any questions concerning your rights as a research participant, you may contact the University of Connecticut Institutional Review Board (IRB) at 860-486-8802.

Consent Form for Participation in a Research Study

Principal Investigator: Benjamin Fuller
Student Researcher: Trevor Phillips
Study Title: Improving Security of UConn

Documentation of Consent:

I have read this form and decided that I will participate in the project described above. Its general purposes, the particulars of involvement and possible risks and inconveniences have been explained to my satisfaction. I understand that I can withdraw at any time. My signature also indicates that I have received a copy of this consent form.

_____	_____	_____
Participant Signature:	Print Name:	Date:
_____	_____	_____
Signature of Person Obtaining Consent	Print Name:	Date:

Debriefing Form for Participation in a Research Study

Principal Investigator: Benjamin Fuller
Student Researcher: Trevor Phillips
Study Title: Improving Security of UConn

Description

Thank you for participating in this study. The purpose of the study is to analyze the security of the UConn Husky OneCard. You were not informed of the purpose of the study ahead of time. Your student ID information and survey results will be stored securely in a locked location by Dr. Fuller, on a UConn owned computer. Your student ID information and survey results will not be publicized. The UConn team is using this information to determine how easy it is to clone or steal a student's ID and privileges. At no point will your information be used to access your account. The researchers are engaged with UConn HuskyOne Card office who are monitoring the researchers' activities. You may withdraw from this study now by not signing below.

We will do our best to protect the confidentiality of the information we gather from you but we cannot guarantee 100% confidentiality. Your confidentiality will be maintained to the degree permitted by the technology used. Specifically, no guarantees can be made regarding the interception of data sent via the Internet by any third parties.

If you have further questions about this study or if you have a research-related problem, you may contact the principal investigator, Dr. Benjamin Fuller at benjamin.fuller@uconn.edu, or the student researcher Trevor Phillips at trevor.j.phillips@uconn.edu. If you have any questions concerning your rights as a research participant, you may contact the University of Connecticut Institutional Review Board (IRB) at 860-486-8802.

Debriefing Form for Participation in a Research Study

Principal Investigator: Benjamin Fuller
Student Researcher: Trevor Phillips
Study Title: Improving Security of UConn

Documentation of Debriefing:

I have read this form and am comfortable with researchers keeping my data. I understand that I can withdraw at any time. My signature also indicates that I have received a copy of this debriefing form. If I choose not to participate at this time, I will return this form unsigned.

_____	_____	_____
Participant Signature:	Print Name:	Date:
_____	_____	_____
Signature of Person Obtaining Consent	Print Name:	Date:

IRB-1 Study Protocol

Protocol Version # and/or Date: Version 2 3-28-2018
Prototol #: H18-009

Study Protocol Title: Security of the Husky OneCard

Clinical Trial/GCP Training

Is this a research study in which one or more human subjects are prospectively assigned[1] to one or more biomedical or behavioral interventions[2] (which may include placebo or other control) to evaluate the effects of those interventions on health-related biomedical or behavioral outcomes[3] (i.e. a clinical trial)? Indicate "yes," "no," or "N/A" in the space immediately below.

No

Is the study fully or partially funded by the NIH? Indicate "yes," "no," or "N/A" in the space immediately below.

No

Have the required key personnel completed Good Clinical Practice (GCP) Training? Indicate "yes," "no," or "N/A" in the space immediately below. (Note that IRB approval will not be given for NIH funded clinical trials until all required key personnel complete the GCP training.)

N/A

Research Plan

Purpose/Introduction:
The purpose of this study is to evaluate the security of the Husky OneCard system. The study is focused on analyzing the ease with which one can obtain information about students from their student ID. Acquisition of such information represents a major security vulnerability. A particular concern is the ability to duplicate a student's card for malicious purposes. A secondary goal of the study is to gather data about participants (admission date, NetID, PeopleSoft number, and birth date) to determine if this data is predictive of the information encoded on student IDs. If this proves to be true, then a student's ID could

[1]The term "prospectively assigned" refers to a pre-defined process (e.g., randomization) specified in an approved protocol that stipulates the assignment of research subjects (individually or in clusters) to one or more arms (e.g., intervention, placebo, or other control) of a clinical trial.
[2]An intervention is defined as a manipulation of the subject or subject's environment for the purpose of modifying one or more health-related biomedical or behavioral processes and/or endpoints. Examples include: drugs/small molecules/compounds; biologics; devices; procedures (e.g., surgical techniques); delivery systems (e.g., telemedicine, face-to-face interviews); strategies to change health-related behavior (e.g., diet, cognitive/behavioral therapy, exercise, development of new habits); treatment strategies; prevention strategies; and, diagnostic strategies.
[3] 3.Health-related biomedical or behavioral outcome is defined as the pre-specified goal(s) or condition(s) that reflect the effect of one or more interventions on human subjects' biomedical or behavioral status or quality of life. Examples include: positive or negative changes to physiological or biological parameters (e.g., improvement of lung capacity, gene expression); positive or negative changes to psychological or neurodevelopmental parameters (e.g., mood management intervention for smokers; reading comprehension and /or information retention, behavioral intervention for psychiatric symptoms); positive or negative changes to disease processes; positive or negative changes to health-related behaviors; and, positive or negative changes to quality of life.

be duplicated with very limited knowledge of the student's personal information. The hypothesis is that (1) yes, student ID information can be acquired easily, and (2) yes, limited personal data can be used to formulate the information encoded on a student's ID.

For EACH Participant Population State the Number of Participants to be Enrolled and Screened, if applicable:
The study will take place over one day and will target UConn undergraduate students passing by a table in the Student Union. Participation is voluntary, we will cap participation at 100 students.

Justification of Sample Size:
In this study, we are not seeking statistical significance; the goal is to correlate student demographics with stored information on the Husky OneCard. Thus, our goal is to maximize participation. Our only limitation is that participation should be high enough to allow verification of hypotheses about how information is stored on the OneCard.

For EACH Participant Population State Describe the Study Population(s):
The only population we consider is UConn undergraduate students. Given this population, the demographics may be very diverse: both genders, all ethnicities and income levels, and a level of education ranging from undergraduate freshmen to seniors. The age range is 18+ (no minors). Thus, we will disqualify participants who are:

1) Under 18.
2) Are not UConn undergraduate students.

Enrollment of UConn Students and/or Employees:
UConn students will be enrolled in the study. UConn employees will *not* be enrolled. The UConn undergraduate student population is necessary to the study because it is the population under consideration. The study is aimed and determining the security of the Husky OneCard system, which is primarily used by *UConn undergraduate students*.

Enrollment of Key Personnel, Spouses or Dependents/Relatives:
Key personnel, spouses of key personnel, or dependents/relatives of any key personnel will not be enrolled in the study.

For EACH Participant Population Describe Recruitment Methods:
Participants will be identified and recruited in the following manner: a table will be set up inside the Student Union near the Game Room for a period of approximately 6 hours. Trevor Phillips will be stationed at the table to solicit participants. First, those who are interested will verbally be asked if they are a UConn undergraduate student and are at least 18 years old. Then, if this is confirmed, Trevor will begin the consent process.

For EACH Participant Population Describe Screening Procedures, if applicable:
For this study, screening will consist of verbal confirmation from the participant that he or she is a UConn undergraduate student and at least 18 years old.

Design, Procedures, Materials and Methods:
A table will be set up inside the Student Union near the Game Room for a period of approximately 6 hours. Research personnel will be stationed at the table to solicit participants. First, those who are interested will verbally be asked if they are a UConn undergraduate student and are at least 18 years old. Then, if this is confirmed, the subject will be asked if he or she "wants to help make UConn a safer campus." The researcher will explain that by swiping the student's ID, he or she will be contributing to raise awareness about making UConn a safer, more secure campus. The student will be provided with the

informed consent form which describes the general goal of improving campus security. This form states that the purpose of the study will be further explained upon completion. Further questions from the subject will be deflected to generalized statements about improving the safety of UConn. Then, if the student swipes his or her ID card, he or she will be asked to complete a survey (via UConn Qualtrics) to gather the following data: birth date, NetID, PeopleSoft number, and admission date. Lastly the researcher will ask the subject if a picture may be taken of the subject, who will hold up a sign which reads, "I helped make UConn a safer campus." The purpose of taking the photograph is to see how willing participants are to have their photo taken. The picture resulting from the photograph will be immediately deleted and not stored long term as part of the study.

This study involves the use of deception. Participants will not be told that the goal of this study is to understand whether OneCards can be duplicated. Deception is necessary for the study because it is intended to measure the ease with which a malicious attacker can obtain arbitrary student ID information. A real attacker would likely use deception to gather this data via a social engineering attack. No reasonable student would give up his or her ID information if they were informed that it will be used for duplicating their Husky OneCard (or in this case, merely obtaining the data represents the *potential* to duplicate a Husky OneCard).

However, participants will be given an informed consent document that will describe what information will be stored and what steps will be taken to secure it. In addition, we will make it clear to participants that participation is voluntary and may end at any time. A unique identifier will be assigned to each participant, starting at 1 and incrementing for each new participant. This unique ID will be linked to survey responses, card information, and photograph; however, the participant's name will not be linked. Upon completion, students will receive a debriefing form. This form informs students about the detailed purpose of the study. Students will be asked to sign this form to indicate continued participation in the study. All participants who do not sign the debriefing form will have their data immediately removed.

Data Analysis:

Data analysis will focus on the relationship between data about a student and the information encoded on the student's ID card. There are 3 "tracks" on the magnetic strip of a student ID card. Track 1 encodes the student's 7-digit PeopleSoft number, so no analysis is necessary here. Track 2 is blank, so again, no analysis is necessary. Track 3 contains a seemingly random code of 14 digits and will be the focus of analysis. The hypothesis is that, rather than being completely randomized, these 14 digits are generated from metadata about a student (such as DOB and admission date).

Analysis will be conducted as follows: Qualtrics survey data will be matched with track 3 data for the corresponding individual. Individuals will be grouped into categories (for example, all students whose birth year ends in '96, or all students who were admitted to UConn in 2016). Then, track 3 data for these groups will be compared digit-by-digit. If, for example, it is discovered that 100% of the time the 4^{th} digit of track 3 is equal to '6' for students admitted to UConn in 2016, we can make a reasonable assumption that the 4^{th} position of the code on track 3 is determined by admission date. Further analysis will be conducted in the same way by grouping respondents into various categories from survey results.

Inclusion/Exclusion Criteria:

There are no inclusion/exclusion criteria except that subjects must be at least 18 years old and must be fully enrolled undergraduate UConn students. A participant may opt to leave the study at any time.

Potential Harms/Risks and Inconveniences:

The potential risks to participants for this study are minimal. The primary risk is that of a breach of information, i.e. participants' student ID information becoming public. With this information, an attacker could theoretically create duplicate student ID cards and use students' Husky Bucks, meal plan swipes and points, and access the student dormitories. However,

construction of a card duplication machine is beyond the capabilities of most individuals. Purchase of a card duplication machine is more likely, but even this typically costs at least $200. From there, the attacker must *also* forge the printed graphics for the student's ID.

Steps taken to minimize risk are as follows: survey data from participants will be gathered securely on the UConn Qualtrics system. Data and photographs of participants who volunteer will be stored on a UConn-owned computer located in Dr. Benjamin Fuller's office, which is locked unless Dr. Fuller is inside. Student ID information gathered from the card reader will also be stored securely on this same computer. This computer has an encrypted hard drive and is only network accessible through the SSH protocol. In addition, the data will be deleted upon completion of the analysis.

Benefits:
There are no direct benefits to participants in this study. However, the hope is that this study will raise awareness about potential security flaws in the Husky OneCard system, which will help the University understand the risks and benefits of the current system.

Risk/Benefit Analysis:
Risk to participants is minimal, and sufficient measures will be taken to safeguard against the unlikely event of confidential student information becoming public. Specifically, data will be stored securely on a UConn-owned computer in Dr. Fuller's office. The benefits are much greater, because discovery of a vulnerability (and the subsequent correction of the vulnerability by the University) improves the safety and security of *all* students at the University of Connecticut. Therefore, the benefits of this study outweigh the risks. Furthermore, the study population is the same group that will receive the benefits from the study satisfying the principle of justice.

Economic Considerations:
There will be no cost to participants except that of time: the study is estimated to take 2-5 minutes to complete. There will also be no financial compensation for students who participate in the study.

Data Safety Monitoring: Survey results will be monitored by the PI in conjunction with the student investigator upon every hour of the study, since it takes place during only one day. Survey responses will be reviewed to monitor for clarity (i.e., the same question is skipped by 5 or more participants). In that case, due to time constrains, the question will not be revised, but future participants will be informed that they should skip the question causing an issue. There is no external sponsor for this research so all problems can be handled internally. In an extreme situation, it may be necessary to consult with the OneCard Office (which is aware of this project). The student researcher will notify the PI of any protocol deviations or adverse events via email and/or phone within one day of their occurrence, and the PI will then notify the IRB via email and/or phone within one work day of receiving this information.

Privacy/Confidentiality Part 1:

Participant privacy will be guarded by assigning a unique ID to each participant which is linked to that participant's survey responses, student card data. This unique ID will *not* be linked to the subject's name. This unique ID will simply be a number starting from 1 and increasing by 1 with each participant. For example, the 5th participant will be assigned the unique ID of 5. As stated above photographs will be immediately destroyed upon being collected. The only purpose of the photograph is to see if individuals are willing to have their picture taken.

Privacy/Confidentiality Part 2: Complete the Data Security Assessment Form:

See the relevant document.

Informed Consent

As PI, you are responsible for taking reasonable steps to assure that the participants in this study are fully informed about and understand the study. Even if you are not targeting participants from "Special Populations" as listed on page 4, such populations may be included in recruitment efforts. Please keep this in mind as you design the Consent Process and provide the information requested in this section.

Consent Setting:
Trevor Phillips will obtain consent. Consent will be obtained at the research setting: a table located in the Student Union near the Student Union Game Room. The study will take place from approximately 10:00 AM to 4:00 PM, so this is when consent will be obtained (i.e., immediately prior to the subject participating in the study). Participants will have as long as they need to make a decision. Privacy of participants will be maintained by not asking for or collecting any personal information of the participants before consent is given. Because of the deceptive nature of the study, participants will be informed of *what* they will be doing prior to the start of the study, but the true motives of the study will be withheld until participants have completed the study.

Capacity to Consent:
Trevor Phillips will exercise his best judgement about whether an individual has the capacity to give consent. He will ensure that participants are fully enrolled undergraduate UConn students and are over the age of 18.

Parent/Guardian Permission and Assent:
No one under the age of 18 will be participating, so this is not necessary.

Documentation of Consent:
The study will collect consent of individuals but this consent involves deception. Specifically, security of the OneCard is not mentioned in the informed consent document. Students will be told the goal of the study is to make UConn more secure. However, students will be informed about what data will be stored and the potential risks of participation. In addition, at the completion of their participation, students will be debriefed as to the true purpose of the study and will be provided an additional opt-out of the study.

Waiver or Alteration of Consent:
We are requesting an alteration of consent to use deception.

- Why is the study considered to be minimal risk?

The study involves the use of a computer for a few minutes and taking a photo. We expect the primary risks from the study to be compromise of personal data. We are taking steps to protect the stored data and view this risk to be minimal.

- How will the waiver affect the participants' rights and welfare? The IRB must find that participants' rights are not adversely affected. For example, participants may choose not to answer any questions they do not want to answer and they may stop their participation in the research at any time.

Participants will still be informed about all data to be collected and the mechanisms being used to protect that data. The only deception is on the purpose of the study. Participants will be informed that they can stop at any time or choose to skip any part of the process. Furthermore, participants will be debriefed to the true purpose of the study and will be provided an additional opportunity to opt out.

- Why would the research be impracticable without the waiver? For studies that involve deception, explain how the research could not be done if participants know the full purpose of the study.

This study crucially involves the use of deception. Participants will not be told that the goal of this study is to understand whether OneCards can be duplicated. Deception is necessary for the study because it is intended to measure the ease with which a malicious attacker can obtain arbitrary student ID information. A real attacker would likely use deception to gather this data via a social engineering attack. No reasonable student would give up his or her ID information if they were informed that it will be used for duplicating their Husky OneCard (or in this case, merely obtaining the data represents the *potential* to duplicate a Husky OneCard).

- How will important information be returned to the participants, if appropriate? For studies that involve deception, indicate that participants will be debriefed and that the researchers will be available in case participants have questions.

Immediately upon completion of the study, participants will be told that the study was designed to understand security of the Husky OneCard.

References / Literature Review:
None

University of Connecticut Office of Research Compliance
Storrs and Regional Campuses

INSTITUTIONAL REVIEW BOARD
RESPONSIBILITIES OF RESEARCH INVESTIGATORS

Responsibilities of Principal Investigators

The IRB holds the PI responsible for the overall management of an approved study. Management of the study encompasses the ethical, technical, administrative, and fiscal elements of a project. The PI may delegate certain tasks, but retains ultimate responsibility and accountability. Principal investigators are required to:

- Acknowledge and accept their responsibility for protecting the rights and welfare of human research participants, including the equitable selection of research participants, ensuring that risks to participants are minimized, and that the risks are reasonable in relation to anticipated benefits,
- Fulfill the training requirement for the protection of human participants in research (CITI on-line training modules, www.citiprogram.org), and to understand the ethical standards and regulatory requirements governing research activities with human participants,
- Supervise all study personnel and ensure that all personnel abide by the ethical principles of respect for persons, beneficence and justice, as outlined in the Belmont Report,
- Ensure that all study personnel are knowledgeable of, and conduct the study in accordance with the approved protocol (including approved amendments),
- Ensure that all research activities have IRB approval and other approvals required by the institution before human participants are involved, and implement the research activity as it was approved by the IRB,
- Report any real or potential conflicts of interests of the PI or any study personnel in compliance with conflict of interest policies and management plans,
- Obtain informed consent from participants before participants are involved in the research, and document consent as approved by the IRB. A copy of the IRB-approved informed consent document must be used. Participants must be provided with a copy of the form after it has been signed, unless the IRB has specifically waived this requirement. Documented evidence of informed consent of the participants or their legally authorized representative is to be retained in a manner approved by the IRB. The consent process involves two required elements: 1) a discussion of the study by the person obtaining consent and the participants, and 2) an opportunity for participants to read the consent form. Please note that it is never appropriate to forgo the discussion, even if participants will then read the consent form. Participants must be given the opportunity to have the consent form read to them if they have difficulty reading,
- Maintain written records of IRB reviews, decisions, research records and informed consent documents,
- Obtain IRB approval for and notify the sponsor (if applicable) of any proposed change to the research protocol *prior to* its implementation, except when necessary to eliminate apparent immediate hazards to the participants,
- Obtain re-approval by reporting progress of approved research to the IRB, in the manner prescribed by the IRB, but not less than once per year,
- Promptly report to the IRB any adverse events, protocol deviations or other unanticipated problems involving risks to participants or others. PIs should not undertake any action with an external funding agency regarding an unanticipated problem or noncompliance without first contacting the IRB Chair or the DRC in order to determine the correct course of action,
- Verify that IRB approval has been obtained from all participating institutions in collaborative activities with other institutions, and that continuing review by other institutions is maintained,

- Ensure the confidentiality and security of all information obtained from and about human participants, and the privacy of participants is maintained,
- Use the most current version of IRB forms and document templates, which can be downloaded from the IRB website (http://www.irb.uconn.edu/forms.html),
- Oversee the budget and expenditures related to the study to ensure that adequate resources are available, including staff, equipment supplies, storage space etc., to conduct the study at the University and any other performance site for which the PI is responsible,
- Ensure charges assessed to insurance carriers are for procedures for illness or injury directly resulting from the research procedures of the study, if applicable,
- Provide the IRB with audit or inspection reports or findings issued by regulatory agencies, cooperative research groups, contract research organizations, the sponsor or the funding agency,
- Communicate, when applicable, the investigator's plans to meet with representatives of the community from which individuals will be recruited, about community concerns, values and expectations,
- Maintain, when applicable, accurate records on the receipt, use and disposition of excess drugs/devices,
- Conduct the study in compliance with internal policies and regulations including 45 CFR 46 and 21 CFR 50 – Protection of Human Participants, 21 CFR 312 – Investigational New Drug Application and 21 CFR 812 – Investigational Device Exemptions; with Good Clinical Practices and, when applicable, 21 CFR 210 – Current Good Manufacturing Practice in Manufacturing, Processing, Packing, or Holding of Drugs and 21 CFR 211 – Current Good Manufacturing Practice for Finished Pharmaceuticals.

Responsibilities of All Key Personnel

The IRB holds all study personnel (including PI and co-investigators) responsible for meeting certain obligations. Study personnel are required to:

- Fulfill the training requirement for the protection of human participants in research (CITI on-line training modules, www.citiprogram.org), and understand the ethical standards and regulatory requirements governing research activities with human participants,
- Comply with applicable IRB policies and procedures,
- Document contact with participants, e.g., obtaining informed consent or informing participants of changes that may affect their willingness to continue participating,
- Provide a thorough explanation of the study in lay terms to the participant during the consent process,
- Provide the participant with an opportunity to ask questions and have them answered when obtaining informed consent and throughout their participation,
- Understand the appropriate use of an investigational intervention (drug or device) as described in the protocol, investigator brochures, product information/drug labeling, and various other available sources such as newsletters, safety alerts, or communications from sponsors, if applicable,
- Be familiar with and follow the adverse event and protocol deviation reporting requirements.